2020-07-21

The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training

Tam, Kimberly

Maritime Technology and Research

https://www.tci-thaijo.org/index.php/MTR

Review Article

The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training

Kimberly Tam*, Kemedi Moara-Nkwe and Kevin D Jones

Faculty of Science and Engineering, University of Plymouth, UK

Article information

Received: April 24, 2020
Revised: June 1, 2020
Accepted: July 2, 2020

Keywords
Cyber range,
Training,
Maritime,
Risk assessment

Abstract

A good defensive strategy against evolving cyber threats and cybercrimes is to raise awareness and use that awareness to prepare technical mitigation and human defense strategies. A prime way to do this is through training. While there are already many sectors employing this strategy (e.g., space, smart buildings, business IT), the maritime sector has yet to take advantage of the available cyber-range technology to assess cyber risks and create appropriate training to meet those risks. Cyber security training can come in 2 forms; the first is so security professionals can raise their awareness on the latest and most urgent issues and increase defense skill levels, and the second form is directed at non-security professionals (e.g., ship builders, crew) and the general public, who are just as affected by cyber threats, but may not have the necessary security background to deal with the issues. Conducting training programs for both requires dedicated computing infrastructure to simulate and execute effective scenarios for both sets of trainees. To this end, a cyber range (CR) provides an environment for just that. The purpose of this paper is to use studies on the concept of cyber ranges to provide evidence for why the maritime sector should embrace this technology for maritime-cyber training, and envision how they will provide maritime risk assessment and raise awareness to combat tomorrow's threats.

1. Introduction

Industries across the world are steadily increasing the integration of technology into their daily operations. The maritime sector, in particular, is embracing new, unique, innovations to improve efficiency and meet opposing demands for just-in-time goods and environmentally friendly travel. Trends of recent security incidences worldwide are showing that, not only is there an increase in the complexity and severity of cyber security threats, there has been a shift from traditional IT (information technology) attacks to infrastructure, which often use both IT and OT (operational technology). Some examples of cyber-attacks on recent infrastructure have affected pipelines (BBC, 2020), centrifuges (Langer, 2011), and even power grids (Lee et al., 2016). Based on the types of systems affected, both IT and OT, it is not unlikely that maritime infrastructure, particularly ports, can be accidently affected or intentionally targeted as well. Unintentional

*Corresponding author: Faculty of Science and Engineering, University of Plymouth, UK
E-mail address: kimberly.tam@plymouth.ac.uk

malware infections have already illustrated the potential disasters, as shown by the Maersk incident (Maersk, 2017), which cost the company at least 200 - 300 M USD.

Training to raise awareness is the first line of defense against cyber and cyber-physical threats, as well as future threats. It trains and helps the public, mariners, and security professionals to be, at least, prepared for and aware of high priority risks and the corresponding mitigation strategies. Using maritime-cyber training programs to train both mariners and security professionals often requires cyber security enabled labs and realistic simulation-based exercises. Generally, this article defines an exercise as using a cyber-security simulation, a sequence of attack and/or defense events, to train trainee participants to have better defensive understanding and mitigation skills against the simulated threats. It is important to note that training participants can be both human and non-human, as artificially intelligent agents could also learn and participate in defense strategies. The similarities and differences of these will be discussed further on. Please also note that this paper uses the phrase *pilot scenario* for a training and awareness activity for IT specialists, mariners, and technical frameworks. Previous studies and iterations of security training exercises have shown that preparing such programs requires a lot of time and resources, with preparation often taking months (Vykopal et al., 2017). This can be a significant dedication of resources, especially when applied to large-scale skill gaps in the cyber sector (Furnell et al., 2017); therefore, the effectiveness of a training program is of high importance.

To meet the demands for these types of facilities and training programs, the concept of a *cyber range* (CR) was born. While a cyber range is physically a series of connected machines, the de facto configuration for many computing environments, conceptually it is a tailored teaching suite with a series of repeatable exercises, monitoring tools, and more. Therefore, software simulation, and diverse training capabilities, are what has drawn so much attention to CRs, and what makes this environment easily customized for different needs. The goal of this paper is to (1) evaluate what has already been achieved to fill the gap in maritime-cyber CR-based training with similar practices and (2) discuss ways to improve CRs for maritime-cyber training for future purposes. More specifically, this paper will build on future CR directions presented in Yamin et al. (2019), focusing primarily on improving scalability, education, and what the paper defines as “federation”. As addressing an issue of this magnitude requires a reasonable amount of time and resources, this work is funded by Cyber-MAR, a European project (Cyber-MAR, 2020). Specifically, the research in this paper was to help meet one of the project objects to enhance the capabilities of cybersecurity professionals and raise awareness of cyber-risks through the use of next generation cyber range environments, and to develop and deploy a highly customizable cyber-risk simulation platform to cover training needs for both mariners and IT professionals. As of 2020, this project is still in the initial development stages, and the specifics of the final product are not set; therefore, this paper is, as previously stated, a more conceptual and generic analysis on how cyber ranges can be used in the maritime context based on previous work on cyber ranges and knowledge of the maritime sector.

The rest of this paper is as follows. In Section 2, cyber ranges designed for other contexts (e.g., space) are shown to illustrate what elements could be successfully used in future maritime-cyber training. This also discusses some of the trends and future needs, identified in previous papers, and how they may lead to better training tools. When appropriate, we shall discuss how Cyber-MAR intends to incorporate the improvements discussed to provide next generation CR-based maritime-cyber training by the end of the project in Section 3. Sections 4 and 5 will examine how these context-specific CRs can be used to improve maritime-based training and risk assessment for both mariners and security professionals in the sector. Section 6 will discuss future work generally, and also more specifically tied to Cyber-MAR’s objectives. This paper concludes with why the maritime sector would conceptually benefit from CR-based training and simulations, and a potential roadmap to raise awareness and improve cyber and cyber-physical safety using the training program and cyber ranges mentioned. For Cyber-MAR project details, please see the Acknowledgements.

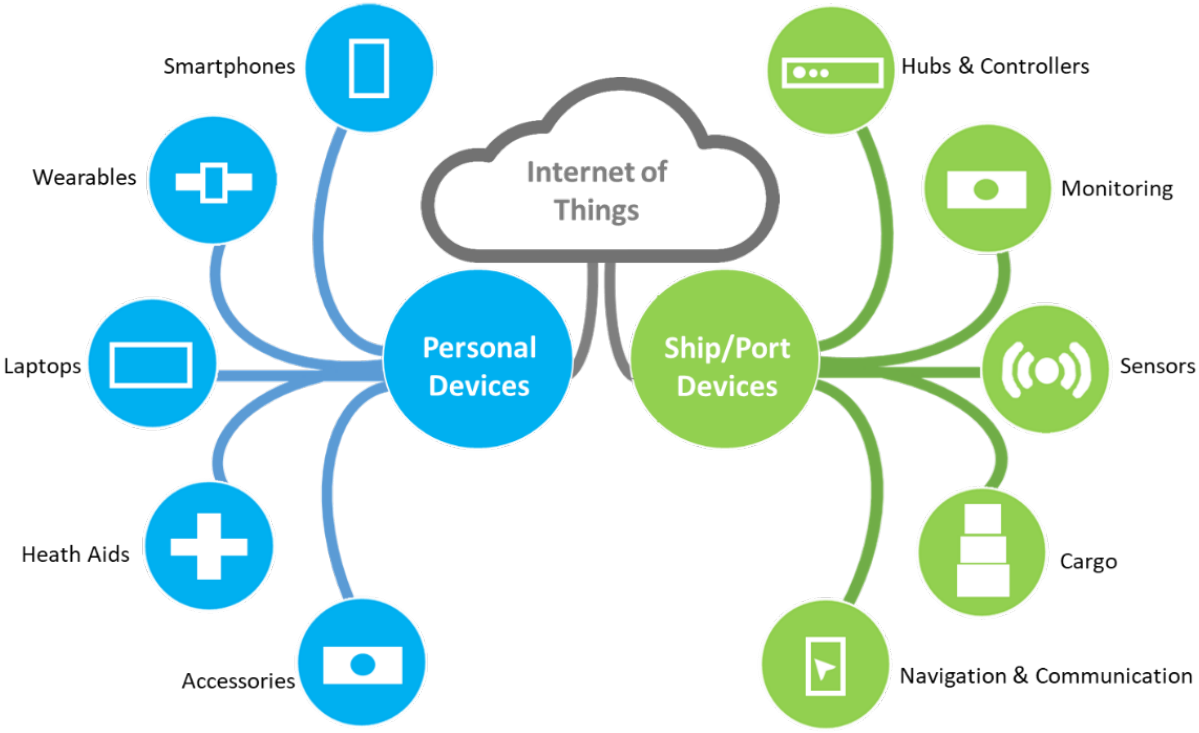

Figure 1 Example information and operation technology (IT/OT) in an Internet-of-Things (IoT).

2. Background

There have been several attempts to classify and structure past uses of cyber ranges and cyber range concepts because of the broad definition and wide number of uses, users, and contexts. One notable attempt was conducted by the Australian government in 2013 (Davis & Magrath, 2013). However, this particular study has several drawbacks today. It was published prior to a considerable increase in cyber range development around 2017 - 2018 and, as a document intended for government audiences, it lacked somewhat in research development discussions. A more recent, and therefore more complete, survey of existing cyber range architecture, design, and use is Yamin et al., (2019). This article provides a comprehensive literature review on several aspects of CRs used globally. General recommendations for the future of CRs are also made in this paper, based on past trends. It is interesting to note that, as of late 2019 when this was published, no notable efforts had been made to use this technology in the maritime context.

Similar to most research in cyber-security areas, much of the current body of research can be classified as IT focused research or OT systems. Operational Technology (OT) is a fairly new term to cover the growing number of SCADA, industrial control systems, and other systems that perform physical operations in addition to cyber. For CR-based training, Siaterlis & Masera (2009) reviewed ranges designed to address the more traditional IT topic of internet security. A large advantage of these studies is to simplify complex systems, like the extensive global internet, into smaller-scale scenarios that testbeds and cyber ranges of all sizes could deal with. While it is best to have a realistic training environment, scalability is also an issue, and discoveries in these more mature areas of research can greatly guide the development of more unusual IT/OT hybrid environments, or even a complex maritime Internet-of-Things (IoT) environment (**Figure 1**).

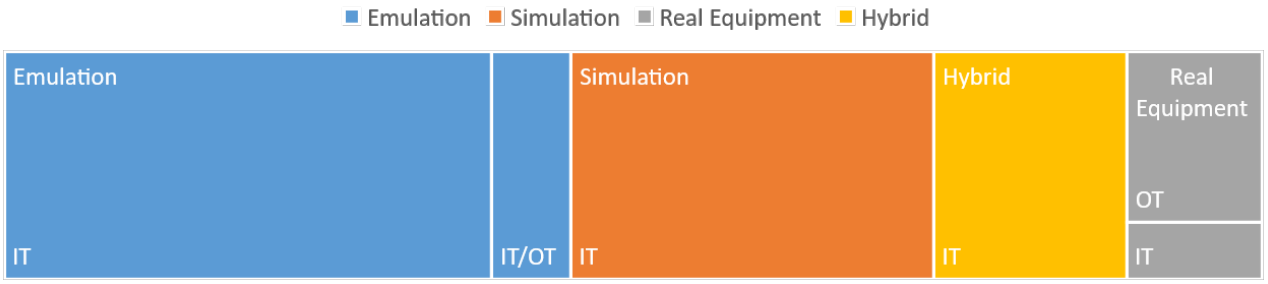

Figure 2 Example information and operation technology (IT/OT) in an Internet-of-Things (IoT).

A survey of more specific SCADA focused testbeds can be found in Qassim et al., (2017). There are many other forms of OT systems but, much like the internet is a significant focus for IT, SCADA is a focus for much OT research. Unfortunately, IT and OT are considered in isolation, and this causes an issue, as many sectors, including the maritime sector, are seeing a convergence of the 2 (Tam & Jones, 2019a). In particular, port infrastructure is becoming smarter and more interconnected with port IT, and both ship bridge and ship engineering are becoming more electronically connected. This changes the nature of potential cyber-attacks and outcomes and, therefore, simulation and training based on the maritime context require a newer hybrid approach. Elements of both IT and OT simulations may also be directly ported into a hybrid environment.

One more aspect to cyber ranges that should be addressed is simulation versus emulation. For instance, most cyber ranges in the public domain can be categorized as either simulation- or emulation-based. There are significant advantages and disadvantages to both approaches, but in general, simulation tend to be valued for high scalability on a small number of servers. In comparison, while emulation is more expensive to implement, the simulations are often more realistic. More generic details between simulation and emulation can be found in other research (Chou et al., 2016). Additional observations on using simulation, emulation, or real systems for researching cyber security in the maritime sector can be found in Tam et al. (2019). Based on research of the 3 options, it seems real systems and environments are better for testing systems and finding attack vulnerabilities, while simulation and emulation are better for scalable, repeatable training programs. For this reason, hybrid simulation and real equipment in a cyber range was chosen as the base technology for Cyber-MAR's human and framework training program. Summarizing several figures and tables from Yamin et al. (2019) into **Figure 2**, we hope to illustrate the rough distribution of CRs using real, simulation, hybrid, or real equipment over the last 18 years. This also shows the proportion of what those CRs were used for, training or research, in IT, OT, or IT/OT areas. What this does not show, however, is that most of the OT and IT/OT orientated CRs were created more recently, since 2014.

In the recent past, cutting-edge cyber range technology, based on simulation, has been produced by NASA to provide training for people manning space stations (Bailey, 2019). The purpose of this was to provide cyberwarfare training and technology development. This simulation-based CR provided NASA with an adaptable virtual environment that represented a typical NASA mission system environment. This setup successfully enabled the training of network defenders and the ability to perform simulated red vs blue training in a space station. While this is pioneering CRs for cyberwarfare in space, Cyber-MAR will be developing equally cutting-edge abilities in the maritime sector, primarily at port, but considering ships as well. Another state-of-the art simulation-based solution for studying industrial control systems (ICS) can be found in Giuliano & Formicola (2019). This focused on raising cybersecurity awareness amongst ICS maintenance staff. Similarly, Cyber-MAR aims to raise awareness in the maritime sector. Just as this research aims to address the lack of cost-effective CRs for the industrial domain, so does Cyber-MAR for the maritime sector. It

is important to note that, although there are commonalities between maritime and space, as well as between maritime and ICS, maritime will need its own unique CR configurations and capabilities, just as space stations and ICS require different CRs.

When considering cyber-physical systems, usually including several OT components, in the last 2 years there has been new research in both emulation (Brownie et al., 2018) and simulation (Kavallieratos et al., 2019). Like in maritime and other transportation sectors (Tam & Jones, 2019b), cyber-physical systems are becoming more popular and a potential risk for cyber and cyber-physical safety. Therefore, the security risk assessment of cyber-physical systems is becoming more and more important. As maritime operations are critical to modern society, with 95 % of world trade depending on the sector (ICS, 2018), it is paramount that cyber ranges in this niche evolve more quickly to meet cyber needs.

3. Cyber ranges and simulation testbeds

The concept of simulating cyber-attacks for research existed before the cyber range concept; one of the earliest papers being Cohen (1999). Despite the age of this study, much of the research content is still relevant, and still applies to current cyber ranges, which are physical testbeds of networked system nodes designed to optimize user experience and teaching capabilities with these simulation and monitoring tools. That said, improving the architecture and tools of a cyber ranges is still a work in progress, especially when applied to new areas, such as maritime-cyber training. In this paper, and the Cyber-MAR project, the aim is to push the state-of-the-art in 3 directions, the maritime context, scalability, and federation, as discussed in the following subsection.

3.1 Maritime context

To achieve the levels of realism necessary to facilitate meaningful training, it is easier to use real equipment, as stated in Section 2. However, this is costly, and hinders both scalability and deployability; therefore, simulation and emulation often provide enough realism, as well as scalability and deployability (i.e., how easy it is to share the training in other areas to other audiences). A hybrid approach with simulation and real data is what Cyber-MAR is using to ensure the project pilot scenarios have the correct degree of real maritime context information. More generally, for the maritime context to be accurately virtualized, several layers of abstraction are likely to need simulating or emulating. This means the simulation needs to consider both digital and physical layers in the maritime sector. In **Figure 3**, we show 3 simplified layers for ports and ships, the main components of the maritime transport sector. Operational technology (OT) tends to exist on the physical layers, including cranes, propulsion, and energy, while IT tends to be placed on higher layers, primarily centered around network packets and operational data. Viewing these layers and understanding how they affect each other has been used previously to simulate and research complex environments, such as smart grids in a city (Park et al., 2019).

In **Figure 3**, the physical layer of the network and energy grids affect the digital layer when it comes to monitoring. Events occurring in communications and logistics will affect the loading and unloading of cargo. Simulating multiple layers for 1 environment can increase overhead and requires a more powerful testbed. One example of SCADA testbeds being designed to be more scalable can be round in Alves et al. (2018); however, that would only be one element of one layer needed to represent a port. For a realistic scenario, not all elements need to be simulated, but **Figure 3** shows several elements that will likely be needed for a simulated maritime environment. Of course, training can limit the number of elements simulated by focusing on a port or ship specifically, or specifically on SCADA networks, as previous studies have done. However, to better understand the overall risks, multiple elements across multiple layers should be simulated and used for research and training purposes. To mitigate the cost of upgrading testbed hardware, scalability is a significant aspect of developing a cyber range.

The maritime sector has a growing need to use CR technology to assess cyber-risks and create appropriate training to meet the risks security people and non-security professionals (e.g., ship builders, crew) face. Conducting effective training in the maritime context is unique and essential due to the unique systems themselves and how they are used at port and at sea.

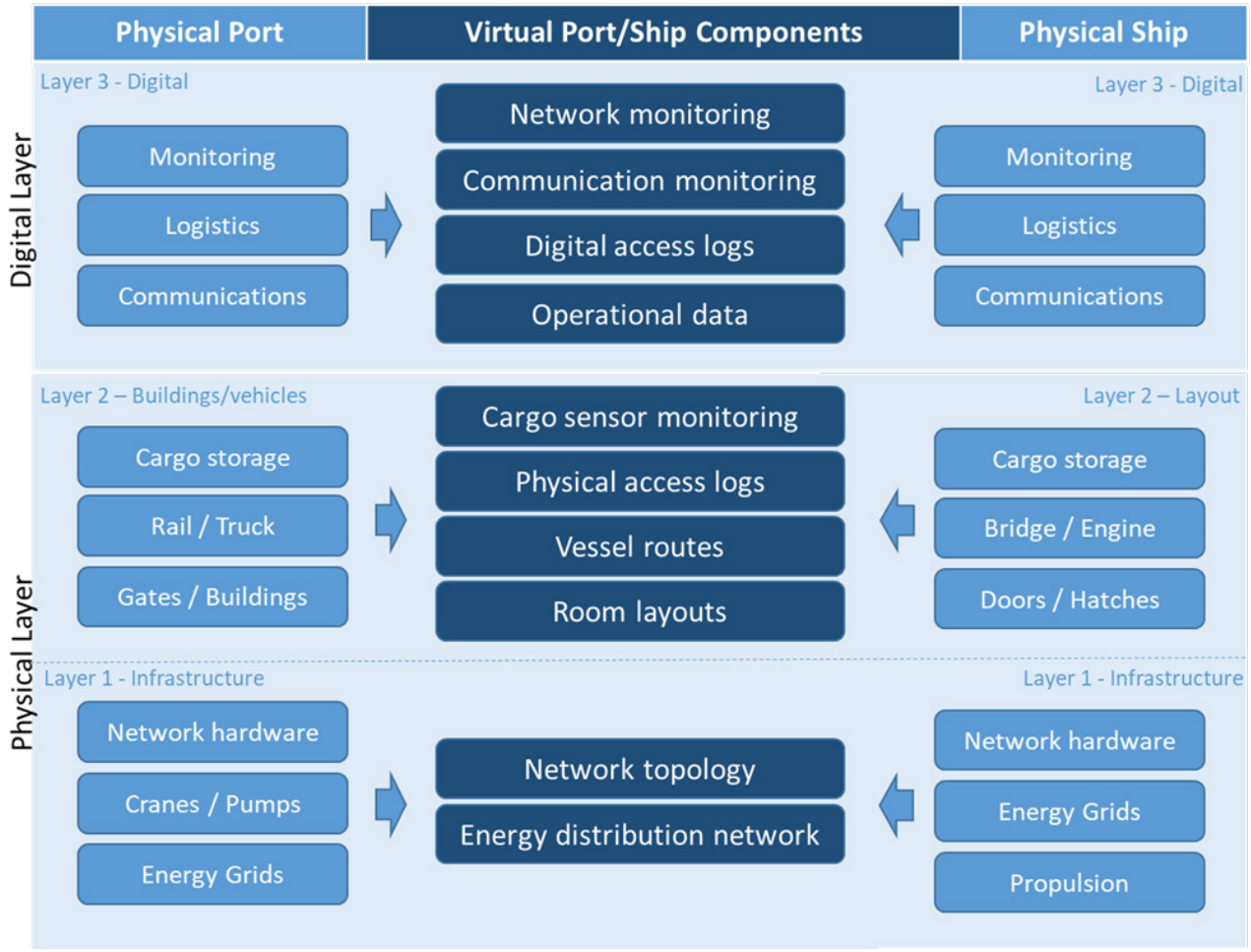

Figure 3 Maritime virtual and physical components for ships and ports categorized into layers.

3.2 Scalability

Often realism, which requires a lot of details, and scalability clash, as it is difficult to scale an exercise as the complexity increases. However, in order to train enough trainees fast enough to counter cyber and cyber-physical risks, CRs need to be scalable to meet demands. More specifically, to achieve the best results from a training exercise, the run time environment mimics the real world as much as possible. As seen with previous small scale and classroom oriented testbeds, this is easily feasible, as scaling the testbed hardware will provide realistic scenarios without noticeable lag. Replay in these smaller environments is also easier, making it easier to train multiple cohorts in a smaller time span. However, as an environment becomes complex, often out of a necessity for more realism, this becomes more difficult. This could be a challenge for cyber-physical training, as it could require several layers of abstraction, as demonstrated in Section 3.1 and **Figure 3**. Given this, a testbed designed to mimic a maritime context will likely require several layers of physical, IT, and OT networks in order to achieve high levels of realism.

Scalability is a common issue when facing real-world use, and there have been several papers researching ways to increase the scalability of cyber ranges in order to improve their usability as efficient training and research tools. Recent examples of new virtualization and emulation techniques being used to increase the scalability of cyber ranges can be found in Beuran et al. (2018), Ficco and Palmieri (2019), Pham et al. (2016). However, increasing the number of virtualized and emulated tools will still continue to add computing burden on the existing hardware and, eventually, the limitations of the physical cyber range or testbed will be reached. This is especially true if simulations are intended to become immersive for the trainees, increasing 3D graphics, the number of actors/players, realistic sensor inputs, and other environment simulations. Minimal infrastructure overhead will also ensure that CRs do not significantly impact the monitor software that collects and analyses trainee performance and simulation data (Hwang & Bush, 2015). A part of scalability is the quantity of data generated and used during a scenario.

As it is may be overly resource taxing for individual sites to continue upgrading their testbed hardware, another option is to begin connecting cyber ranges in order to pool computing resources, and also share simulation, monitoring, and training capabilities. This is the approach Cyber-MAR is attempting, connecting cyber ranges in different physical locations using VPNs in order to improve scalability and support a higher level of realism. The 3 scenarios of this project will include a mixture of manual and human-generated input, much like most training scenarios. In most scenarios, and in the case of Cyber-MAR, not all data will be generated by human interaction and, in fact, data generators will be used to increase realism and improve the program's capability for repeating exercises in a scalable way. **Table 1** shows different types of data that can be seen in a cyber range and, more importantly, how scalable they may be. While "scalability" refers to how scalable the scenarios (i.e., data gathering, generating, monitoring, and processing) are, storage also affects scalability because of the limitations (e.g., memory, processing) of the physical testbed.

Table 1 Types of data found in a cyber range during a simulation-based training program, and how realistic, scalable, and storage intensive they each are.

	Realism	**Scalability**	**Storage**
Stubs: Data to meet minimum requirements, often fixed replies to allow other services to function	Low	High	Low
Fuzzing: Data simulate all types of input for a system, but do not apply logic on applying inputs	Medium	Medium	Low
Simulation: The more realistic data is, the lower scalability tends to be, because it is challenging to accurately simulate many components together	High	Low	Low
Replay: Data can be replayed after being captured from human use, real devices, or other simulations. These are fixed event sequences	High	Low	High

3.3 Federation

Lastly, we wish to discuss a method to improve launching realistic training exercise scalability within range to specifically address cyber-security in the maritime context, which is, as explained, unique. One term for this is *federation*, which was mentioned in papers like Yamin et al. (2019), Hwang and Bush (2015) to share activities, explore portable aspects, and compose cyber range capabilities on demand by connecting ranges. These aspects of cyber ranges and testbeds have not been addressed as much as scalability; however, they are becoming more sought after. Examples of federation include support for running simulations and actives (i.e., training, research)

over multiple locations. The connection of multiple physical testbeds in several areas for one, connected cyber range could aid in both scalability and federation. Cyber-MAR aims to connect 3 physical testbeds, one of which is also portable. Therefore, while the portable component may lack the computing power itself required for high levels of realism, when federated to other larger, but stationary, testbeds, it is conceptually possible to achieve all 3 desirable traits mentioned in this article. Apart from the hardware aspect of a cyber range, individually or a connected collection of them, another way to ensure a training program is easy to share and deploy is to develop standard pilot scenario descriptions and definitions (Edgar & Rice, 2017). As a complex environment to simulate and train a range of users in maritime-cyber security, CRs for maritime training may require federation to achieve scalability and realism.

As mentioned earlier, a federated cyber range can be implemented in a number of ways. This could include 1) an entirely simulation-based setup, 2) a purely emulated set-up, 3) a pure real-life system setup, or 4) some combination of all of the above process imitation methods. A complex environment, such as a port, is often made up of a large number of sub-systems, and the choice of process imitation method that best suits a particular sub-system depends on a wide variety of factors, including the nature of the sub-system and the sub-system behaviors that are of highest interest. If the cyber range needs to be highly scalable, then simulated components often need to make up a large share of the final cyber range, as discussed in Section 3.2.

A simulator can run in simulated time, whilst emulators are often restricted to running in real time. This can be a significant factor to consider, because some system behaviors of interest might manifest over long periods of time, and they therefore might need to resort to using simulated time in order to investigate the system effects caused by these system behaviors and/or events. Others might need to sync with other systems. A key example of this is the investigation of the propagation of worms in a computer, worms in a computer network, and associated effects. A worm might propagate through a large enterprise network very slowly, and so using simulated time is often necessary in order to make the experiment practical. This can be done by, for instance, simulating the network in a discrete event network simulator, such as ns-3 (NS-3, 2020).

In other cases, it may be more appropriate for a more realistic model based on the emulation of networked computing devices. This can help identify system effects which could be very difficult to investigate in a purely simulation-based environment, such as vulnerabilities which are due to flaws in the implementation of security protocols as opposed to vulnerabilities inherent in the security protocols themselves. Due to the fact that a maritime port is made up of many different autonomous or semi-autonomous systems devoted to a wide variety of tasks, different cyber effects would be of interest, depending on the system in question and the nature of the cyber effects one wishes to investigate. This dictates whether simulation, emulation, or real testing is most appropriate, and why a federated cyber range, one made up of many largely autonomous subsystems, would be appropriate for investigating a complex system like ports and complex ships.

4. Training

This section will discuss context-specific cyber ranges that can be used to improve maritime-based training for both mariners and security professionals in the sector. While the underlying simulations and emulations may be very similar at a technical level, to make sure the training programs are effective for professionals of both maritime and security backgrounds, the amount of exposure to the details of the scenario may be different. Referring back to **Figure 3**, different levels of abstraction may be more relevant for training mariners, and IT specialists may require more detail of internet levels, both internal and internal, for monitoring and detection, in order to maximize learning. Issues on realism, particularly around bespoke protocols, and scalability have been discussed previously, and affect how accurate and usable training exercises are. However, the trainee learning and education aspects are achieved differently (Bertram, 2020b; Subasu et al., 2017; Caliskan et al., 2017). In addition, the type of data used during a training

scenario should ideally be simulated. While some stub data can be used (**Table 1**), only using stub data would lack realism. Fuzzed and replay data will also not be ideal since this will ignore live input from the trainee. It is critical for training simulators to react to trainee actions and input, and this will be implemented in the cyber range outputs of the Cyber-MAR project.

In Tam and Jones (2019a) a survey on cyber-security was conducted to understand the risks and the type of training individuals have had. Roughly 32 % of the responses were seafarers, 19 % were higher management and IT security managers, and the remainder were classified as ship owners, manufacturers, students, and others. In this survey, participants named the standards of training as the biggest problem in the maritime industry (74.6 %), with cybercrimes and cyber-attacks the second biggest issues (55.2 %). In addition, 60.7 % said they had not received any cyber-security related training, but that they believed maritime-specific cyber-security training would be useful for their daily tasks (75 %). This is ranked higher than generic IT cyber-security training. Conducting training programs for both security specialists and mariners requires dedicated computing infrastructure to simulate, potentially with multiple layers (**Figure 3**), and execute effective scenarios for all sets of trainees. To this end, a cyber range provides an environment for just this. Furthermore, federating multiple physical testbeds to form one cyber range with extra capabilities would increase training scalability and realism. While the cyber range technology will support the training scenarios (e.g., environment, storyline, actors, monitors), the training program must also be supported by scoring and management capabilities to facilitate learning during exercises.

Facilitating learning can be used to enhance problem solving skills (John, 1989; Pham et al., 2016; Vykopal et al., 2017). To help teach, scoring mechanisms and other ways of measuring performance are often used to help trainees learn. This has been used for student training in technology and simulation-based mariner training (Chiou et al., 2009; Marine Board, 1996). More recently, and applied to cyber security training in cyber ranges, studies like Huang et al. (2015) have begun developing specific scoring mechanisms. More generally, to help facilitate learning for security experts and mariners in the new developing area of maritime-cyber training, training and scoring mechanisms can be classified by the method used, and the tools used.

1) Cyber range training methods can be classified by whether the performance scoring is based on achieving specific objectives or by analyzing logs generated as the scenario is played out. One example of a maritime-cyber specific objective, or flag, may be successfully executing an operation, like a change in course, despite cyber-interference. This would be more beneficial in CR-based cyber-physical training (Tam & Jones, 2018), whereas more cyber-security orientated training may benefit more from evaluating logs (e.g., system, network, intrusion detection/prevention) to judge performance.

2) Apart from method, training tools can be classified as software- or hardware-based. These tools are what are actually required for the exercise trainers to view flags (i.e., flag type, success, fail), log analyzers, and anything else required for the scenario. This relates back to virtual, emulated, or real hardware additions to a CR. For maritime-cyber training, this is highly dependent on the training scenario, and requires future research and trials.

5. Maritime-cyber IDS and risk assessment

It is important to note that “training” can be applied to more than human trainee participants, as artificially intelligent agents can also learn cyber defense and mitigation strategies. Data obtained from monitoring the scenarios played can be used to improve models for other simulations. In Cohen (1999), the approach used various simulations, or pilot scenarios, that were modelled using attacker and defender skills as key parameters. Attackers were classified extensively and based on real attackers, making simulation more comprehensible and increasing training efficiency. Models such as these can help automate or speed-up analysis and detection. This is becoming more important, as the number of cyber threats grow as skill shortages continue (Furnell et al., 2017).

While scenarios are run in a CR for trainees, monitoring data can also be fed into machine learning algorithms and other types of intrusion detection and risk assessment tools. For example, Cohen (1999) simulated cyber-attacks and defenses and produced data such as duration of the attack, if successful, and the outcome. With machine learning, this data can be used to train systems for better mitigation, recovery, and general awareness of the issues (e.g., risk assessment).

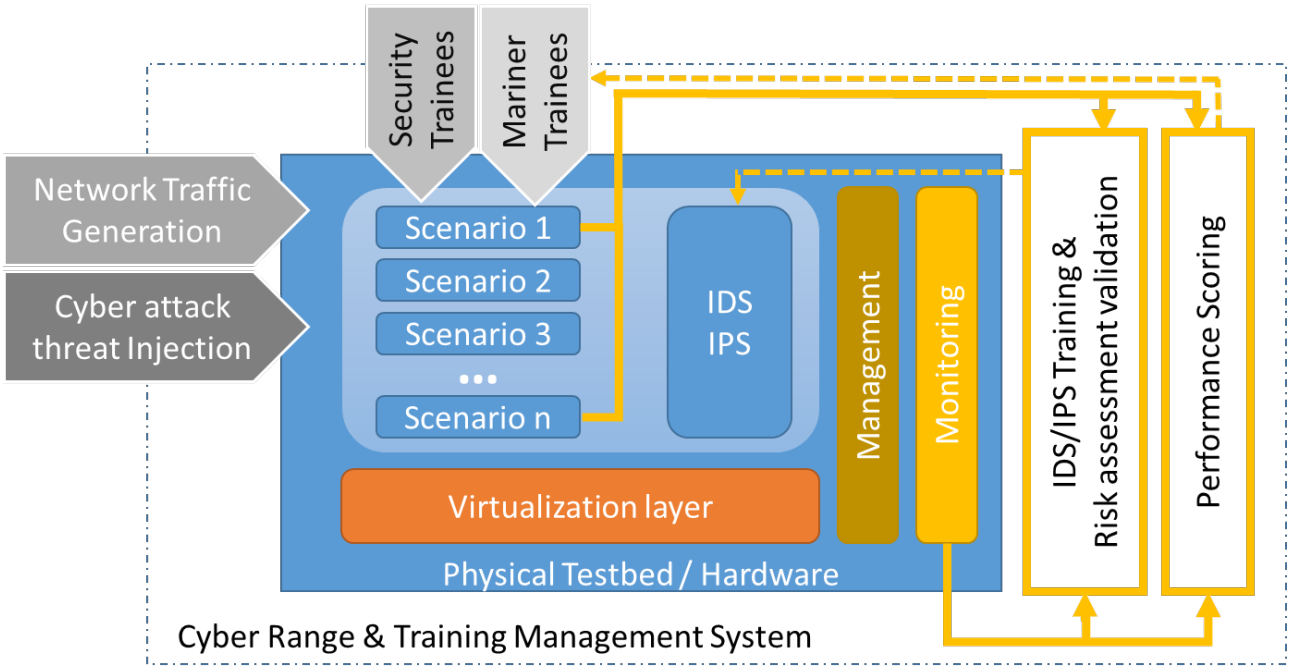

Figure 4 CR for training security and mariner trainees and IDS/IPS/Risk assessment tools.

Intrusion detection systems and intrusion prevention systems (IDS/IPS) in a cyber range can be used to monitor a network of systems for malicious activity or violations of policy. The definition of "malicious" is determined by the security architect and the training data used. As shown in Haider et al. (2017), using CR technology can greatly increase the amount of useful data that can be used to improve realistic IDS/IPS systems. Therefore, collecting data that is generated during a number of training scenarios can increase realistic IDS/IPS and realistic maritime-cyber risk assessment (**Figure 4**). Like with IDS, the downside with many risk assessment models is they struggle with the lack of realistic data. Papers like Cohen (1999) have raised concerns that that many attack simulation models are rarely validated against real world scenarios and data. In Svilicic et al. (2019), quantitative cyber risk analysis was done with a crew interview and a computational vulnerability scanning of a ship's Electronic Chart Display and Information System, one of several bridge systems, but one often critical to ship operations. Furthermore, this study was validated with real world data from a university training ship, making it a valuable piece of work. Alternatively, the framework MaCRA is a dynamic risk assessment framework for multiple maritime systems, across ship and port, designed specifically for maritime-cyber issues (Tam & Jones, 2019a) and, while it has used some real data, it would greatly benefit from data extracted from cyber range training exercises. Not only will there be more system-level and human reaction statistics that can be used to increase the validity of cyber-risk assessments, the repeatability of the experiments will allow for higher confidence. Part of the real world data validation will also be provided with CERTs and CSIRTs, by engaging with at least 2 CERT/CSIRT teams. There are Cyber-MAR partners that

are CERTs and, at a later stage, additional teams will be invited to get involved in training simulations and risk analyses.

6. Future work

It is clear from maritime technology trends that cyber security is a growing risk in the industry (Bertram, 2020a). Systems in ports and on ships are becoming more complicated, integrated, and even automated, although to different degrees. Training the industry and developing new technical solutions to improve cyber security and awareness of the issues are critical going forward. In this paper, we identified one potential solution, using cyber ranges to train security specialists, mariners, and systems. This is to help raise awareness, increase risk mitigation, and improve strategies for threat detection, prevention, and recovery. However, the use of cyber ranges for these types of problems have only recently begun to be applied seriously, with the highest time of activity being the last ten years (2010 - 2020) (Yamin et al., 2019). As highlighted by many studies, the realism and scalability of cyber range solutions still have room for improvement. While some studies have focused on improving certain cyber range capabilities (see Section 3), others have explored using the technology for specific problems. This includes, but is not limited to, cyberwarfare and cyberwarfare in space stations (Hwang & Bush, 2015; Bailey, 2019). In a similar fashion, this paper has explored the potential uses of cyber ranges for the maritime sector. However, there are several areas of future research to be explored, some of which are currently being researched by the European project Cyber-MAR, details in the Acknowledgements. In this paper, we classify the areas of future cyber range development to address maritime-cyber issues into 4 categories; 1) enhancing physical testbed capability, 2) introducing and improving the realism of the pilot scenarios played in the CR, 3) effective training for both security experts and mariners, and 4) data for increasing the realism of IDS/IPS and risk assessment frameworks.

6.1 Testbed hardware and components

There are 2 areas of future work on the physical cyber range testbed that we wish to discuss. Firstly, CRs can be connected to increase processing power, particularly if the cyber-range will be simulation or emulation intensive (Yamin et al., 2019). However, on the flipside, this will increase bandwidth and security issues, such as confidentiality. Therefore, any new bandwidth or cybersecurity issues will need to be addressed concurrently. Secondly, creating a physical and simulation hybrid CR by introducing real systems into the range can dramatically increase the realism, but may cause issues in repeatability (Tam et al., 2019). The benefit of either of these methods would be to improve the capabilities of the cyber range. This primarily increases realism but could also increase teaching and monitoring capabilities. In the maritime sector, this is particularly important, as one scenario could either require a complex environment to replicate or require several levels of details (**Figures 3 - 4**) in order to train different trainees. In particular, it is important to consider the training needs for mariners, security professionals, those at sea, and those at port. If the maritime sector begins to use cyber ranges to raise awareness and train people in maritime-cyber mitigation strategies, this will likely push the state-of-the-art for testbeds, cyber ranges, and cyber-physical scenarios (simulation, emulation, hybrid). Development of the physical CR is important in determining the advancements discussed in 6.2 and 6.3 as well.

6.2 Improving scenario simulation and training

Another area for improving the state-of-the-art to be more appropriate for training maritime cyber security would be to improve the simulation as well as the teaching methods. This is an important area for future research, as the teaching needs of security IT and mariners operating on ships or at ports differ. It is important to research if one, detailed, multi-layered scenario (**Figure 3** and **Table 1**) is better than two tailored scenarios for security professionals and mariners, particularly if the two groups see different parts of a larger cyber incident, or as maritime and

traditional security issues continue to converge. As the area of maritime-cyber continues to evolve, and as cyber range solutions evolve as well, there are many possibilities in this area. Specific to the mariner aspect, it would be interesting to see if it possible to incorporate maritime-cyber CR-based training into simulation-based navigation training, which most navigators undergo anyway for other training. This area of research could benefit from, and assist in, other transportation-based research for air, rail, and car, as well as industrial control systems. Depending on the layers simulated or emulated, there may also be parallels between smart grids or cities and other infrastructure.

As training material is produced and trialed, the project will ensure that IMO training regulations, guidelines, and practices such as IMO (2017 and IMO (2013) will be complied. An exhaustive list is outside of the scope of this paper, as by the time the project has progressed to providing and evaluating training, regulations may have been changed or amended. This is possible as maritime cyber policy evolves, seen in similar, relevant, provisions in the International Safety Management Code (IMO, 2013). This includes training guidance for roles under ISM code and risk management. Cyber-MAR training will be designed to increase awareness through practical and re-playable exercises for the trainees, but also for viewers and readers of the outputs of the exercises. The next section describes more methods to increase awareness of risks with cyber ranges.

6.3 Improving realism of IDS/IPS and risk assessment

Lastly, aside from human trainees, we discuss how the outputs of a cyber range training pilot or simulation can be used to improve cyber-security related software. For example, the outputs of cyber-attack and defense simulations include the duration of the attack and the eventual outcome (Cohen, 1999). This data can be fed into other models. In the Cyber-MAR project, the outputs of the cyber-risk models (e.g., MaCRA) are then considered inputs for an econometric model to then calculate the risk in terms of potential economic loss. While MaCRA was initially designed to provide more detailed outcomes beyond “win”/”lose”, future work within Cyber-MAR is also estimating the duration of the attack and the effects of the attack. Project partners will use this data to calculate the econometric outcomes. This is often a missing element in risk assessment, and it is difficult to discuss cyber-risks with larger organization without underlining the financial risks and concerns. Data taken from the training experience, particularly pilots that have been repeated many times with a range of trainees, will provide some much needed statistics in this area, as well as feed machine learning algorithms designed for defense and protection mechanisms. This can include network or host-based intrusion detection and prevention mechanisms (Ring et al., 2019). Future research in this area will provide useful cyber security intrusion detection and prevention tools that are maritime sector appropriate and designed to aid the personnel within the sector at different levels (mariner, ship builder, security manager, etc.). Ideally, these can be integrated with existing equipment to detect and prevent cyber intruders. Some alterations may be required, but the basic IDS/IPS rulesets may also be used at ports and on ships.

7. Conclusions

In this paper we discussed how and why the maritime sector would conceptually benefit from cyber range-based training and simulations. Just as other sectors have embraced CR solutions, if applied to the maritime sector, a potential roadmap could be provided to raise awareness and improve cyber and cyber-physical safety using the training methods and technical solutions mentioned. If implemented correctly, and with some future advancements in research, cyber ranges could provide good defensive strategies against evolving cyber threats and cybercrimes. In particular, this paper discussed using CR solutions to raise awareness and use that awareness to prepare technical- and human-based mitigation and defense strategies. While there are already many sectors employing this strategy, the maritime sector has yet to take advantage of the available cyber-range technology to assess cyber-risks and create appropriate training to meet those risks. As discussed, cyber security training appropriate for this sector can come in two forms; 1) security

professionals who can raise their awareness on the latest and most urgent issues and increase defense skill levels, and 2) non-security professionals (e.g., ship builders, crew) and the general public, who are just as affected by cyber threats but may not have the necessary security background to deal with the issues. We have discussed why conducting training programs in CRs requires dedicated computing infrastructure to simulate and execute effective scenarios for both sets of trainees. Although some future research is needed to ensure that the CR hardware, architecture, training capabilities, and outputs are beneficial, we conclude that the concepts associated with CR maritime security solutions could have significant, positive, effects on maritime-cyber security and are worth exploring fully. As the project progresses, trainee feedback will be collected after CR training exercises, and surveys will be conducted with experts to determine the exact effectiveness of methods.

Acknowledgements

This paper is a part of the research efforts under Cyber-MAR. The Cyber-MAR project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 833389. Content reflects only the authors' views, and the European Commission is not responsible for any use that may be made of the information it contains.

References

Alves, T., Das, R., Werth, A., & Morris, T. (2018). Virtualization of SCADA testbeds for cybersecurity research: A modular approach. *Computers & Security, 77*, 531-546. doi:10.1016/j.cose.2018.05.002

Bailey, B. (2019). *NASA IV&V's cyber range for space systems.* NASA.

BBC. (2020). *Ransomware-hit US gas pipeline shut for two days*. Retrieved from https://www.bbc.co.uk/news/technology-51564905

Bertram, V. (2020). Technology trends for ships and shipping of tomorrow. *Maritime Technology and Research, 2*(1), 1-18. doi:10.33175/mtr.2020.190783

Bertram, V., & Plowman, T. (2020). Digital training solutions in the maritime context: Options and costs. *Maritime Technology and Research, 2*(2), 52-68. doi:10.33175/mtr.2020.190782

Beuran, R., Tang, D., Pham, C., Chinen, K. I., Tan, Y., & Shinoda, Y. (2018). Integrated framework for hands-on cybersecurity training: CyTrONE. *Computers & Security, 78*, 43-59. doi:10.1016/j.cose.2018.06.001

Brownie, A., Watson , S., & Williams, W. (2018). Development of an architecture for a cyber: Physical emulation test range for network security testing. *IEEE Access, 6*, 73273-73279. doi:10.1109/ACCESS.2018.2882410

Caliskan, E., Tatar, U., Bahsi, H., Ottis, R., & Vaarandi, R. (2017). *Capability detection and evulation metrics of cyber security lab exerciese*. In Proceedings of the 12th International Conference on Cyber Warfare and Security, Air Force Institute of Technology, Dayton, Ohio, USA,

Chiou, C. K., Hwang, G. J., & Tseng, J. (2009). An auto-scoring mechanism for evaluating problem-solving ability in a web-based learning environment. *Computers & Education, 53*(2), 261-272. doi:10.1016/j.compedu.2009.02.006

Chou, T. S., Baker, S., & Vega-Herrera, M. (2016). *A comparison of network simulation and emulation virtualization tools.* In Proceedings of the ASEE Conference & Exposition, New Orleans.

Cohen, F. (1999). Simulating cyber attacks, defences, and consequences. *Computers & Security, 18*(6). doi:10.1016/S0167-4048(99)80115-1

Cyber-MAR. (2020). *Cyber-MAR: Cyber preparedness actions for a holistic approach and awareness raising in the Maritime logistics supply chain*. Retrieved from https://www.cyber-mar.eu

Davis, J., & Magrath, S. (2013). *A survey of cyber ranges and testbeds. Technical Report. Defence Science and Technology*. Cyber and Electronic Warfare Division, Edinburgh, Australia.

Edgar, T., & Rice, T. (2017). Experiment as a service. In Proceedings of the 2017 IEEE International Symposium on Technologies for Homeland Security. Waltham, MA, USA. doi:10.1109/THS.2017.7943470

Ficco, M., & Palmieri, F. (2019). Leaf: An open-source cybersecurity training platform for realistic edge-IoT scenarios. *Journal of Systems Architecture, 97*, 107-129. doi:10.1016/j.sysarc.2019.04.004

Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security, 2017*(2), 5-10. doi.org/10.1016/S1361-3723(17)30013-1

Giuliano, V., & Formicola, V. (2019). *ICSrange: A simulation-based cyber range platform for industrial control systems.* Retrieved from https://arxiv.org/abs/1909.01910

Haider, W., Hu, J., Slay, J., Turnbull, B., & Xie, Y. (2017). Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling. *Journal of Network and Computer Applications, 87*, 185-192. doi:10.1016/j.jnca.2017.03.018

Huang, Z., Shen, C. C., Doshi, S., Thomas, N., & Duong, H. (2015). Cognitive task analysis based training for cyber situation awareness. *IFIP Advances in Information and Communication Technology, 453*, 27-40. doi:10.1007/978-3-319-18500-2_3

Hwang, N., & Bush, K. (2015). *Operational exercise integration recommendations for DoD cyber ranges*. Technical Report 1187, Lincoln Laboratory, Massachusetts, USA.

ICS. (2018). *Review of maritime transport*. In Proceedings of the International Chamber of Shipping, United Nations Conference on Trade and Development. Geneva, Switzerland.

IMO. (2013). *ISM Code and Guidelines on Implementation of the ISM Code.* Retrieved from http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx

IMO. (2017). *International Maritime Organization (IMO-MSC) (2017) Maritime cyber risk management in safety management systems.* Retrieved from http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution MSC.428(98).pdf

John, S. (1989). Cognitive technology: Some procedures for facilitating learning and problem solving in mathematics and science. *Journal of Educational Psychology, 81*(4), 457-466. doi:10.1037/0022-0663.81.4.457

Kavallieratos , G., Katsikas, S., & Gkioulos, V. (2019). *Towards a cyber-physical range.* In Proceedings of the 5th on Cyber-Physical System Security Workshop. Auckland, New Zealand

Langer, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy, 9*(3), 49-51. doi:10.1109/MSP.2011.67

Lee, R., Assante, M., & Conway, T. (2016). *Analysis of the cyber attack on the Ukrainian power grid*. Washington DC: E-ISAC.

Maersk. (2017). *A. P. Moller Maersk improves underlying profit and grows revenue in first half of the year*. Retrieved from https://edit.maersk.com/en/the-maersk-group/press-room/press-release-archive/2017/8/a-p-moller-maersk-interim-report-q2-2017

Marine Board. (1996). *Simulated voyages: Using simulation technology to train and license mariners*. Washington DC: National Academic Press. doi.org/10.17226/5065.

NS-3. (2020). *Network simulator*. Retrieved from https://www.nsnam.org

Park, S., Lee, S., Park, S., & Park, S. (2019). AI-based physical and virtual platform with 5-layered architecture for sustainable smart energy city development. *Sustainability, 11*(16), 4479. doi:10.3390/su11164479

Pham, C., Tang, D., Chinen, K. I., & Beuran, R. (2016). CyRIS: A cyber range instantiation system for facilitating security training. In Proceedings of the 7th International Symposium on

Information and Communication Technology (pp. 251-258). Ho Chi Minh City, Vietnam. doi:10.1145/3011077.3011087

Qassim, Q., Jamil, N., Abidin, Z. I., Rusli, E. M., Yussof, S., Ismail, R., Abdullah, F., Jaafar, N., Hasan, H. C., & Duad, M. (2017). A survey of SCADA testbed implementation. *Journal of Science and Technology, 10*(26), 1-8. doi:10.17485/ijst/2017/v10i26/116775

Ring, M., Wunderlich, S., Scheuring, D., Landas, D., & Hotho, A. (2019). A survey of network: Based intrusion detection data sets. *Computers & Security, 86*, 147-167. doi:10.1016/j.cose.2019.06.005

Siaterlis, C., & Masera, M. (2009). *A review of available software for the creation of testbeds for internet security research*. In Proceedings of the 1st International Conference on Advances in System Simulation. Porto, Portugal. doi:10.1109/SIMUL.2009.33

Subasu, G., Rosu, L., & Baboi, I. (2017). *Modeling and simulation architecture for training in cyber defence education*. In Proceedings of the 9th International Conference on Electronics, Computers and Artificial Intelligence doi:10.1109/ECAI.2017.8166396

Svilicic, B., Kamahara, J., Matthew, R., & Yoshiji, Y. (2019). Maritime cyber risk management: An experimental ship assessment. *Journal of Navigation, 72*(5), 1108-1120. doi:10.1017/S0373463318001157

Tam, K., & Jones, K. (2018). Maritime cybersecurity policy: The scope and impact of evolving technology on international shipping. *Journal of Cyber Policy, 3*(2), 147-164. doi:10.1080/23738871.2018.1513053

Tam, K., & Jones, K. D. (2019a). *MaCRA: A mModel-based framework for maritime cyber-risk assessment*. Technical Report. WMU Maritime Affairs.

Tam, K., & Jones, K. D. (2019b). Situational awareness: Examining factors that affect cyber-risks in the maritime sector. *International Journal on Cyber Situational Awareness, 4*(1), 40-68. doi:10.22619/IJCSA.2019.100125

Tam, K., Forshaw, K., & Jones, K. D. (2019). *Cyber-SHIP: Developing next generation maritime cyber research capabilities.* In Proceedings of the International Conference on Marine Engineering and Technology. Oman. doi:10.24868/icmet.oman.2019.005

Vykopal, J., Oslejsek, R., Celeda, P., Vizvary, M., & Tovarnak, D. (2017). *KYPO cyber range: Design and use cases*. In Proceedings of the 12th International Conference on Software Technologies. doi:10.5220/0006428203100321

Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security, 88*, 101636. doi:10.1016/j.cose.2019.101636